What's New for FortiMail 5.2.0

What's New for FortiMail 5.2.0

September 2, 2014

1st Edition

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Fortinet Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

What's New

FortiMail 5.2.0 GA release is one of the FortiMail major releases, which comes with many new features and enhancements. This document lists the following ones:

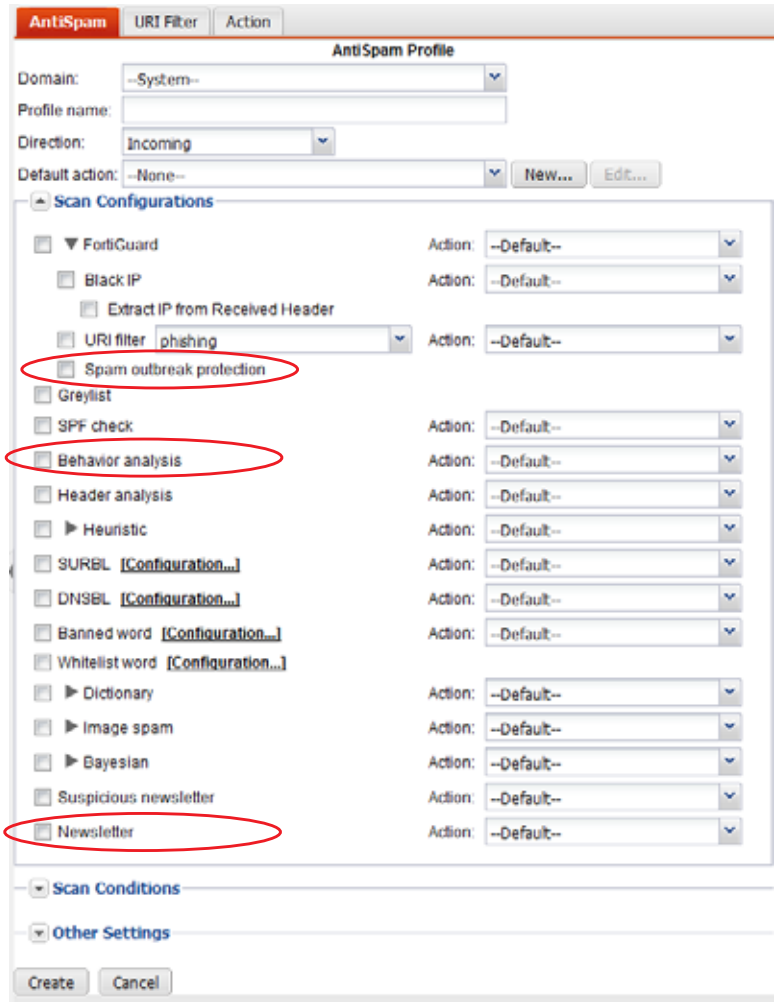
- New VM platform support
- New antispam features
- Integration enhancement with FortiSandbox
- LDAP group in ACL rules
- URI exempt list
- Digitally sign outbound email with S/MIME
- MX record support in mail routing rules
- LVM support on FortiMail VM
- New server mode features
- Content profile query on LDAP server

New VM platform support

In addition to VMware VSphere Hypervisor ESX/ESXi virtual machines, FortiMail VM 5.2.0 can now be installed on Microsoft Hyper-V servers. For more information, see the FortiMail VM (Hyper-V) Install Guide on docs.fortinet.com.

New antispam features

A few new antispam techniques have been added to 5.2.0 release to combat spam. These features are in the antispam profile settings under *Profile* > *AntiSpam* > *AntiSpam*.



Spam outbreak protection

When there is a spam outbreak, FortiGuard antispam service may need some time to update its database. In this case, FortiMail can hold the suspicious email for a short period of time before it query the FortiGuard server for the second time.

To configure how long FortiMail will hold email before query FortiGuard for the second time, use this CLI command (note that this can only be configured with the CLI command):

```
config system fortiguard antispam
  set outbreak-protection-period <minutes>
end
```

The default interval is 30 minutes.

Behavior analysis

To improve spam catch rate, FortiMail uses the text part and HTML part of the email body to analyze the similarity of uncertain email against those well-known spam messages which are received recently.

Newsletter detection

Although newsletters and other marketing campaigns are not spam, some users may find them annoying.

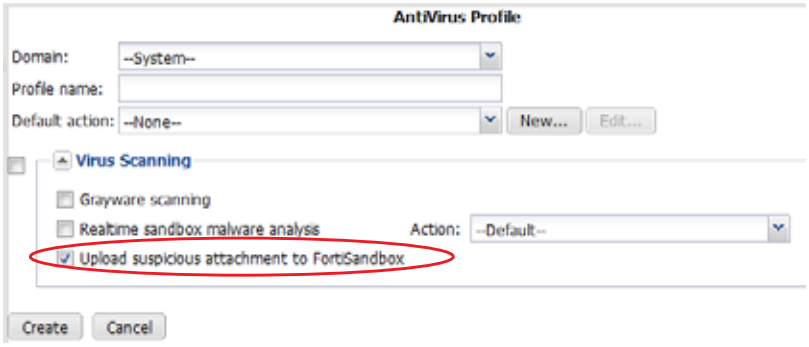
Enable detection of newsletters and select an action profile to deal with them. For example, you can tag newsletter email so that users can filter them in their email clients.

Integration enhancement with FortiSandbox

Integration with FortiSandbox has been enhanced to combat Advanced Persistent Threat (APT). Email is queued while suspicious files are sent to FortiSandbox for evaluation. After receiving query results from FortiSandbox, FortiMail will take actions that are defined in the relevant antivirus action profiles.

This feature is in the antivirus profile settings under *Profile* > *Antivirus* > *Antivirus*.

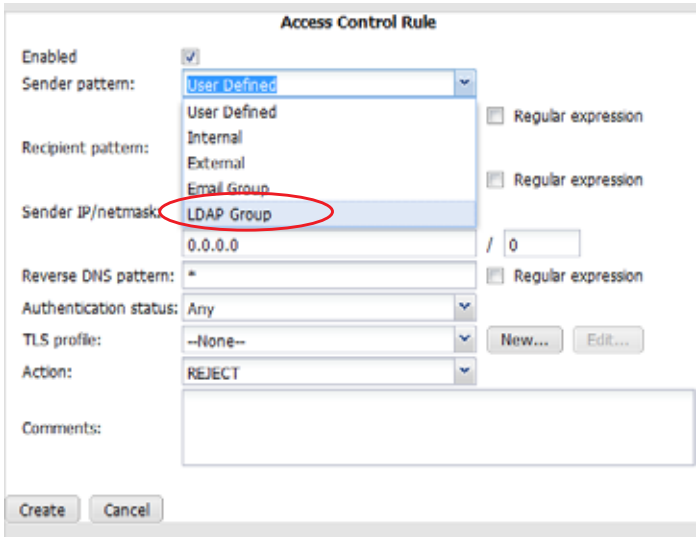
Figure 1: FortiSandbox integration



LDAP group in ACL rules

The user patterns now support LDAP groups under *Policy* > *Access Control* > *Receiving*.

Figure 2: LDAP group support in ACL

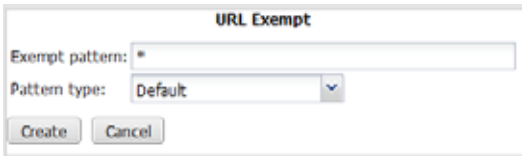


URI exempt list

In case a good URL is misconfigured and assigned to a spam category in the URI filter (under *Profile* > *AntiSpam* > *URI Filter*), you can correct the problem by specifying the URLs to be exempted from scanning and blocking.

To do this, go to *AntiSpam* > *URL Exempt List* > *Exempt*. The patterns can contain wild cards or regular expressions.

Figure 3: URL exempt list



Digitally sign outbound email with S/MIME

In addition to encryption, FortiMail can now sign the outgoing email with S/MIME.

This feature is added under *Profile* > *Encryption* > *Security* > *Encryption* and *Encryption* > *S/MIME* > *Certificate Binding*. When you configure an access control delivery policy, you can use the encryption profile.

Figure 4: Sign action in encryption profile

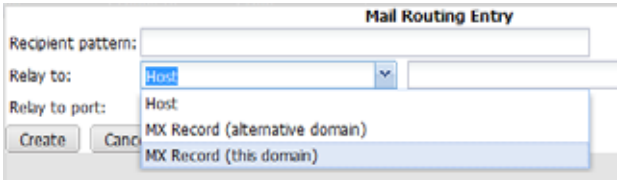
Figure 5: Sign action in certificate binding

MX record support in mail routing rules

The mail routing under *Profile* > *Session* > *Mail Routing* is part of the advanced MTA control features. By default, this feature is hidden. To enable it, use the following CLI command:

```
config system global
  set mta-adv-ctrl-status enable
end
```

Figure 6: MX record in mail routing



LVM support on FortiMail VM

The following CLI commands have been added to support the logical volume manager (LVM) on the FortiMail VM platforms.

```
execute lvm enable/disable
execute lvm extend
execute lvm summary
```

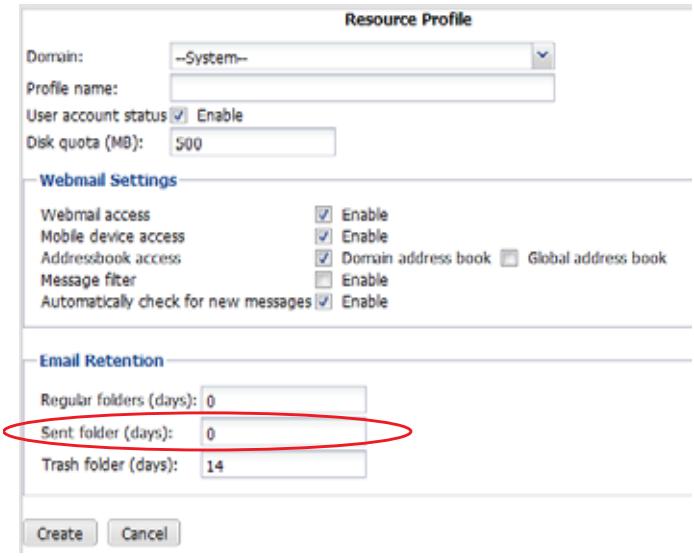
New server mode features

Several server mode feature have added to this release.

Email retention for sent email

Under *Profile* > *Resource Profile*, you can now configure the retention time for the sent email. The default value is 0, which means not to delete email.

Figure 7: Sent email retention



Email address automatic completion in webmail

When composing email in webmail, automatic address suggestions from the address book will be displayed while you are typing.

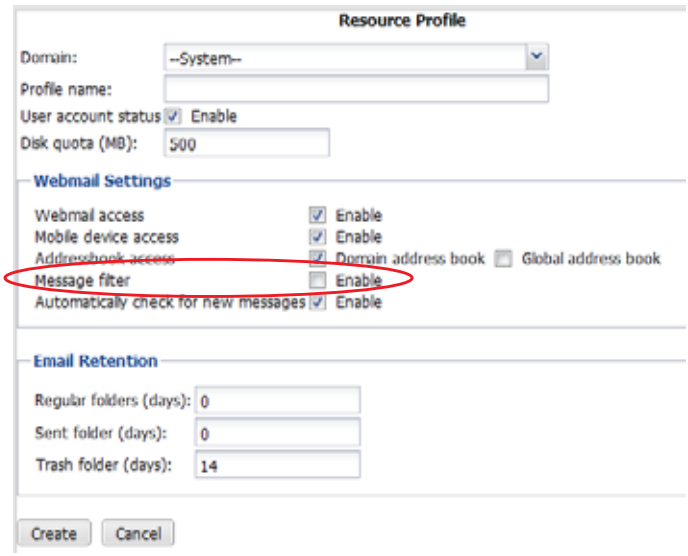
CardDAV support

In addition to WebDAV and CalDAV services, FortiMail now supports CardDAV calendar sharing service.

Email filter in webmail

In the resource profile settings under Profile > Resource > Resource, you can enable the message filter so that the webmail users will be able to set up filter rules under their preference settings. If not enabled, the webmail users will not be able to use this feature.

Figure 8: Message filter contro on admin GUII

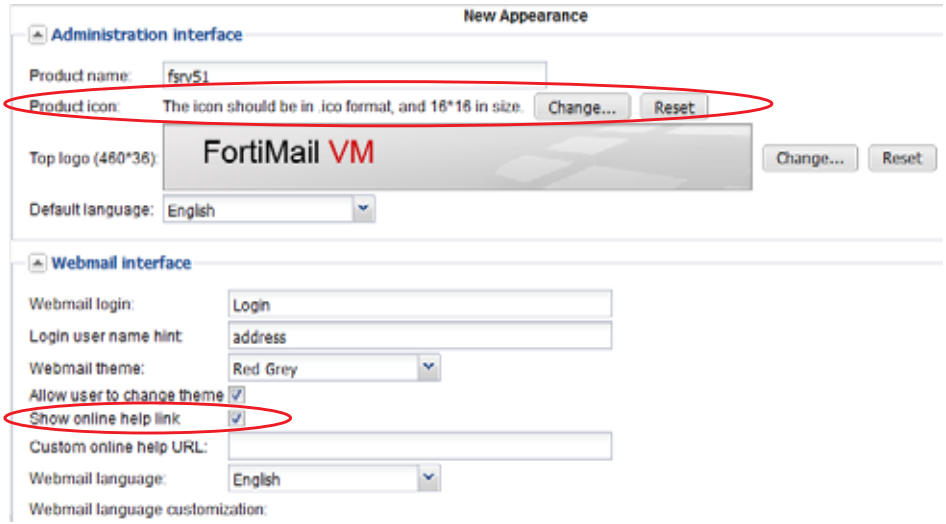


Favicon and webmail help customization

Under *System* > *Customization* > *Appearance*, you can now upload your own favicon image.

You can also choose not to show the online help link in the webmail. This might be useful if you do not want to show the help contents provided by Fortinet.

Figure 9: Favicon and online help customization



Content profile query on LDAP server

In the LDAP profile settings under *Profile* > *LDAP*, you can now choose to retrieve the content profile from the LDAP server. Only antispam and antivirus profiles can be retrieved before.

Figure 10: Content profile query